AU/ACSC/0217/97-03

# INTERNATIONAL LAW

# HOW IT AFFECTS RULES OF ENGAGEMENT AND RESPONSES IN INFORMATION WARFARE

A Research Paper

Presented To

The Research Department

Air Command and Staff College

In Partial Fulfillment of the Graduation Requirements of ACSC

by

Major Robert D. Miller

March 1997

# Report Documentation Page

| Report Date | Report Type | Dates Covered (from... to) |
|---|---|---|
| 01MAR1997 | N/A | - |

| | |
|---|---|
| **Title and Subtitle**<br>How it Affects Rules of Engagement and Responses in Information Warfare | **Contract Number** |
| | **Grant Number** |
| | **Program Element Number** |
| **Author(s)**<br>Miller, Robert D. | **Project Number** |
| | **Task Number** |
| | **Work Unit Number** |
| **Performing Organization Name(s) and Address(es)**<br>Air Command and Staff College Maxwell AFB, Al 36112 | **Performing Organization Report Number** |
| **Sponsoring/Monitoring Agency Name(s) and Address(es)** | **Sponsor/Monitor's Acronym(s)** |
| | **Sponsor/Monitor's Report Number(s)** |
| **Distribution/Availability Statement**<br>Approved for public release, distribution unlimited | |
| **Supplementary Notes** | |
| **Abstract** | |
| **Subject Terms** | |
| **Report Classification**<br>unclassified | **Classification of this page**<br>unclassified |
| **Classification of Abstract**<br>unclassified | **Limitation of Abstract**<br>UU |
| **Number of Pages**<br>47 | |

## Disclaimer

The views expressed in this academic research paper are those of the author(s) and do not reflect the official policy or position of the US government or the Department of Defense.

## *Contents*

*Page*

## *Illustrations*

*Page*

## *Preface*

This research examines an area that only within the last several years started receiving attention from civilian and military leaders—the legal details of information warfare (IW). The legal aspects concerning IW are only now starting to mature and will require refining as we encounter IW scenarios. As a result, I found this research effort a challenging and interesting endeavor as it expanded my knowledge and expertise in an area of interest to me personally and professionally. Although only touching on one aspect of a huge area of interest in today's military, my hope is this research will serve to encourage others to continue to analyze the nuances embedded in IW and come to find, as I did, that this is a complex, wide open area requiring much more thought and development.

I wish to thank Major Michael Foster, my research advisor, for his dedication and guidance during this effort. Also, Lt Col Wilson Crafton for his assistance and the constant, valuable flow of material on IW he provided throughout this research. I cannot forget the members of seminar 36 who provided the support, stimulating interaction, and camaraderie throughout the year—thanks!

And last, but definitely not least, I wish to thank my wife Lorraine and son Joshua, for their tremendous support and tolerance during this research effort. I cannot thank them enough for the sacrifices they made and the love they gave.

## *Abstract*

The importance of reliable, timely information to the success of military operations, while precluding an adversary from accessing information, has been known since wars began. Today, a combination of electronic devices, such as computers and sensors, are creating an "information age" that redefines how we conduct military operations. A major challenge to decision makers and military leaders is to understand the impact of international laws in the information age and its influence on rules of engagement (ROE), and response development. By all accounts, our dependence on information and information systems will continue to grow along with technological advances, enhancing our own command, control, communications, computer, and information capabilities, while also increasing our vulnerabilities. As a result, a key issue our decision makers and military leaders must be aware of concerns the legal considerations in using IW and in responding to IW threats and attacks. Developers of our ROE must provide the guidance for legally, appropriately responding to IW attacks, while ensuring the right to self-defense. Our leaders must also devise appropriate response options against foreign powers conducting IW operations against the US. We must base responses on the level of threat to our national interests, while considering intent, international law, and elements such as proportionality and necessity inherent in the Law of Armed Conflict.

# Chapter 1

# Introduction

> *In order to win victory we must try our best to seal the eyes and ears of the enemy, making him blind and deaf, and to create confusion in the minds of the enemy commanders, driving them insane.*
>
> —Mao Tse-tung
> On the Protracted War (1938)

Arguably the biggest area of interest and discussion in the United States military today, information warfare (IW) and its importance to the successful prosecution of military operations, has been recognized for millennia. The value of information is a function of the information's reliability and timeliness. From a military perspective not only is reliable, timely information critical to the success of an operation, but the ability to preclude an adversary from gathering information is equally critical to the warfighter. In my view, there are three primary reasons the topic is receiving such interest. First, the speed with which technology is changing and the enhancements being made provide tremendous capabilities to maximize information gathering; however, they also provide adversaries those same advances and advantages. Although armies throughout history recognized the value of information, major differences between militaries of today and the past are: (1) amount and speed information is gathered and disseminated, (2) its impact on a commander's situational awareness and battlefield knowledge, and (3) the new vulnerabilities it presents.

Armies from the beginning of warfare could gather and disseminate information only as fast as an individual could travel and horses could gallop. As a result, information could be days, weeks, or months old when it reaches the user. With the onset of the industrial age, inventions such as the telegraph and telephone greatly improved information gathering and dissemination. This increased the speed users received information, reduced dissemination time to hours or minutes, and significantly expanded the area of coverage a commander could "see." Today, computers, electronic mail, and the development of the Internet not only provide a quantum leap in the speed with which information moves, but it is now cheaper to obtain and accessible to more people.1 Figure 1 provides a general depiction of how the speed and amount of information increased over the millennia. By some estimates, over the next 20 years, the amount of information available will increase a 1000-fold over current amounts and capabilities.2

However, as information capabilities increased, the dependence of warfighters on information also grew and with it, so did the vulnerabilities. For adversaries seeking to exploit these vulnerabilities, IW provides an attractive alternative to many adversaries who cannot afford the high costs of developing, maintaining, and using advance weapons.3 Additionally, regardless of their technical sophistication, an adversary can now remotely, yet significantly, affect another country's interests by "hacking" or injecting viruses into their computer systems, or devising other "techno-geek" styles of IW. And, to make matters worse, easy to use automated tools for breaking into

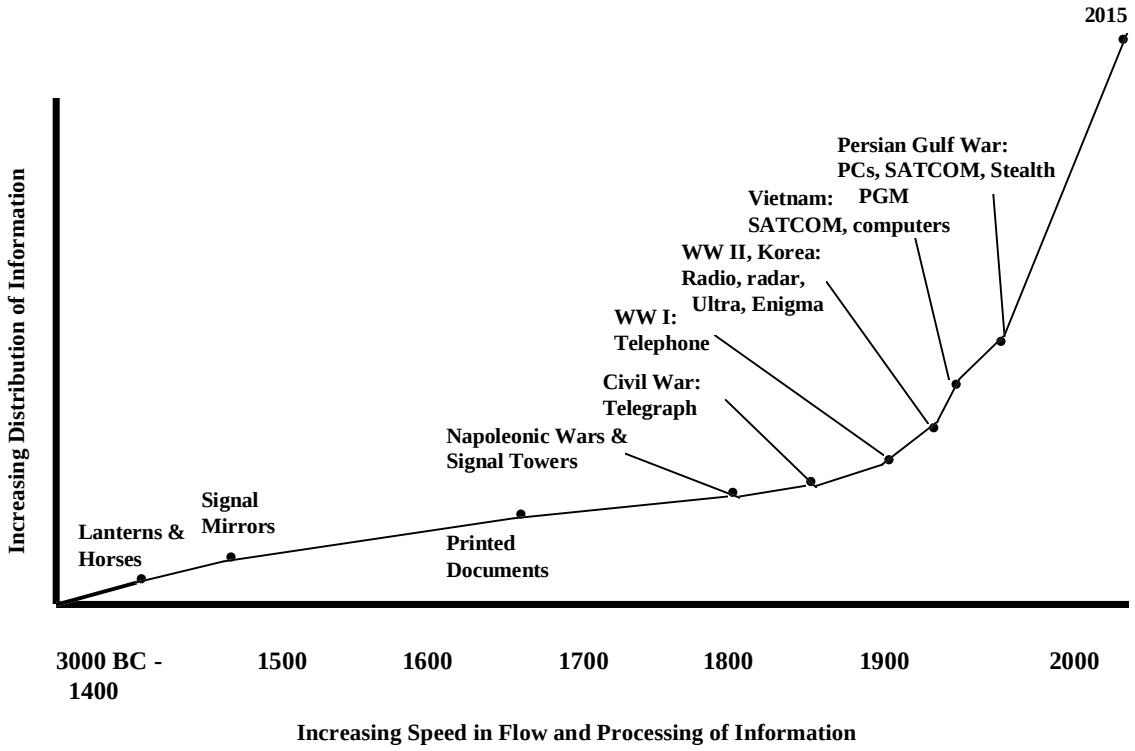


**Figure 1. Increasing Access to Information**

computers, and current information on computer software security flaws are now readily available on the Internet.[4]

A second reason for the increased interest in IW is as the military continues to downsize, information technology is a force multiplier of tremendous potential and must be exploited to the maximum extent possible. General Colin Powell summarized the situation as: "A downsized force and a shrinking defense budget result in an increased reliance on technology, which must provide the force multiplier required to ensure a viable military deterrent." Additionally, in describing the importance of information systems in the Gulf War, he points out that, "Battlefield information systems became the ally of the warrior. They did much more than provide a service; personal computers were force multipliers."[5]

The third reason for the increased interest in IW has to do with the overwhelming success of coalition forces in the Gulf War and the contributions information played in the success of this conflict. The coalition's ability to use information to their advantage, while denying the Iraqi military access not only to their information capabilities, but access to friendly information, blinded Saddam Hussein and his military to coalition intentions. Within minutes of the outbreak of hostilities, coalition forces had removed the Iraqis' ability to effectively coordinate operations, while coalition forces had near real time access to information and situation reports due to satellite, airborne, and a myriad of other information assets. The impact of IW on military capabilities was profound and it highlighted the force multiplying effect information dominance can have. However, it also amplified the fact that a skillful, purposeful adversary can employ IW against us and turn these positive impacts around to seriously disrupt our military capabilities.

As a result, not only has technology greatly enhanced the ability to gather reliable information quickly, but the challenges to protect friendly information from an adversary increased significantly. For these reasons, the literature is filled with debates defining what IW is, what it entails, and why it is important. However, the topic has now reached a level of maturity and gathered enough advocates who embrace the concept and its associated value that a next logical step is to discuss what is legal from an IW standpoint and how do we effectively respond to IW efforts by adversaries. Questions are being asked about the legalities of using IW, what impact these legalities have on the guidance we provide our military, and what is an acceptable response to an adversary caught waging IW on our financial, political, or military computer systems. The weapons of IW, from destroying an adversary's command and control capabilities to injecting a virus into a

computer system, have the potential to disrupt and create a level of chaos and confusion every bit as dramatic as that created by weapons of mass destruction--nuclear, biological, and chemical.

Therefore, this paper will focus on what I believe is an important next step to the myriad of IW literature, how does international law affect the development of rules of engagement and possible responses to IW activities by an adversary or rogue state? I will begin by briefly discussing the progression of IW from a historical perspective, looking at several examples to highlight how technology has increased the volume and speed of information dissemination. Next, I will detail some of the threats that currently exist or are in development to highlight the serious consequences of failing to properly understand and react to IW's destructive potential. I will next discuss the importance of rules of engagement and the influence of international law on their development. Finally, I will discuss some possible responses to dealing with incidences of IW using Dr. Karl Magyar's Core-Intermediate-Peripheral Model as well as key considerations to developing responses. Because of the sheer scope and complexity of the IW arena, I will confine my discussion to IW and its impact from a military prospective. However, we should recognize IW can be waged in a non-hostile environment against civilian targets as well, with similar catastrophic effects. Adversaries and terrorists of today represent a very real IW threat and, as they become more sophisticated in their use of IW weapons and techniques, the more widespread their possible sphere of influence. As General Downing states, "If you consider the terrorist act as an act of war against you, then you have a tremendous range of options available to you. To defeat terrorism, to keep it under control, we need to bring the power of the US government to bear--all agencies."[6]

## Notes

[1] Steven Lubar, *Infoculture* (Boston: Houghton Mifflin Co., 1993), 17.

[2] Seminar lectures, Joint Operations course, ACSC, Maxwell AFB, AL, AY97.

[3] US Department of Defense, *Report of the Defense Science Board Task Force on Information Warfare-Defense*, Washington, DC: Office of the Under Secretary of Defense (Acquisition and Technology), (November 1996): 2-4.

[4] Ibid., 2-4 and 2-15.

[5] General Colin L. Powell, "Information-Age Warriors," *Byte 17*, (July 1992): 370.

[6] Bill Gertz, "Terrorism and the Force," *Air Force Magazine 80*, no. 2 (February 1997): 71.

# Chapter 2

# A Historical Look at Information Warfare

> *The history of command can thus be understood in terms of a race between the demand for information and the ability of command systems to meet it.*
>
> —Martin Van Creveld, Joint Pub 6-0
> From *Command in War,* Harvard University Press, MA. 1985

The criticality of having information about an adversary, while denying them access to information about friendly forces, is a principle recognized by military and civilian thinkers since man engaged in organized warfare. Over the centuries the speed we gathered and disbursed information radically changed as technology improved. Early information-gathering efforts were primarily via word of mouth, by calvary, or by runners. As a result, from a military perspective, the information gathered was primarily of value at the tactical level, that is individual battles or engagements. As technology improved, the speed, depth, and timeliness of information significantly increased, as did the warfighter's dependency on it.

## The Agrarian Age

An early example of the use of IW and its effect on a military campaign occurred during Hannibal's efforts to defeat the Romans during the Second Punic War. Having just

defeated the Roman army at the Battle of Trebia, Hannibal decided to rest his men during the winter and replenish his army. During this period, he used his well-established spy network in Italy to gather intelligence about the Romans and their army.[1] Armed with this intelligence, Hannibal outmaneuvered the Romans, cutting off their lines of communications. Also, being well-versed in Roman military practices and his Roman counterpart's tactics, he set up an ambush at Lake Trasimene.[2] Achieving complete surprise, Hannibal annihilated the Roman army, despite being greatly outnumbered.

The Mongol armies of the twelfth and thirteenth centuries also utilized IW to enhance their abilities to defeat their enemies. Using a network of horsemen known as "arrow riders," they kept their commanders informed about nearby enemy movements.[3] Additionally, they recognized the need to deny their enemy situational awareness and as a result, specifically targeted enemy communications capabilities, such as enemy messengers. Their tactics and intimate understanding of the importance of information to their military success permitted the Mongols to decisively defeat much larger armies.

## The Industrial Age

With the dawn of the Industrial Age, the speed, reliability, and value of information greatly increased as inventions, such as the telephone and telegraph, found their way into military use. One of the first uses of the telegraph appeared during the Civil War as Union forces used technology to reduce the time needed to gather and distribute information. General Grant believed to achieve a military victory required the use of all available resources and technology at a nation's disposal. As Grant stated, "War is progressive because all instruments and elements of war are progressive."[4] In fact, so critical did the

Union view the value of information that after the First Battle of Bull Run the government seized all telegraph systems and incorporated them into the new Military Telegraph Service.[5]

However, the Confederates also recognized the value of information gathering and dispersal as well as denying information to the enemy. In one instance, a Confederate officer realized he could cause confusion in the Union military by tapping into their telegraph lines and impersonating them; for hours he listened to Union transmissions and input erroneous information.[6] As a result of this innovative use of IW, both sides recognized the need to protect their information gathering and dissemination capabilities and developed encrypted codes to guard their important messages.

Although communications capabilities remained crude, information technology continued to advance, ultimately leading to the development of radios and radars and the resulting increased use of these inventions by the military.[7] The use of radios greatly magnified the field commander's abilities to control armies throughout larger areas of operations by eliminating the requirement to be linked by wire. This resulted in tremendous increases in speed of communications between units and provided commanders near real-time situational awareness. However, there was a price to pay for this increased efficiency and speed: increased vulnerability of interception by the enemy. During World Wars I and II, there were numerous examples of the impact IW had on the outcome of those conflicts. In World War I, for example, the French were intercepting German radio transmissions and receiving German radiograms as quickly as the intended recipients. During the course of the war, estimates show the French intercepted more than 100,000,000 words.[8]

One of the most famous uses of IW involved the Allies breaking the German's naval Enigma code during WWII. The interception and breaking of the coded messages between Admiral Doenitz, commander of Hitler's submarines, and his U-boats provided the Allies with information about the locations and movements of Germany's U-boats and allowed the Allies to redirect their convoys and sink Germany's subs.[9] The fundamental importance of this use of IW lies in the fact the Battle of the Atlantic was critical to both sides winning the war and by breaking the Enigma code, the Allies were able to win this battle and ultimately, the war.

Vietnam marked another leap in speed of information-gathering capabilities and availability. During the Vietnam War, satellites and computers were used for the first time,[10] resulting in more information being made available quicker, via satellite reconnaissance, and providing commanders with perspectives of the battlefield not previously possible. With this tremendous increase in information quantity and speed came the problems of processing and protecting it. However, information technology improvements did not stop here; the use of IW during the Gulf War provided the impetus for the recent interest about IW.

## The Information Age

Some have called the Persian Gulf War the "first information war."[11] Although this statement is debatable, the influence information and information systems had on the outcome of the conflict is not. The impact information systems had on the way this conflict was fought, coordinated, and executed was profound. From the initial strikes on Iraqi command and control facilities to make blind and deaf the Iraqi war machine, to the

use of computers, satellites, airborne command and control assets, and deception throughout the conflict, information operations significantly influenced the outcome.

However, as previously mentioned, with the tremendous increases in information gathering and dissemination capabilities came the corresponding increase in the ability of an adversary to engage in IW and affect another country's well being, regardless of their technical sophistication. An excellent example of this occurred during the US involvement in Somalia. Despite limited finances, the Somali clan leader, Mohammad Farah Aideed, used IW to keep the US guessing. He succeeded in winning the information war, and ultimately achieving the objective of removing the US from Somalia, by using well-deployed, highly maneuverable intelligence forces along with techniques such as bouncing cellular phone and radio transmissions off city walls to confound US attempts to locate the sources of these transmissions.[12]

As the above shows, IW is not a new idea; however, the amount of information available and dissemination speed changed dramatically over the centuries. Military thinkers always recognized information's value, but the depth and timeliness of information available today greatly increased access, perspective, and unfortunately, threats to information security. As a result, even the most technologically impaired adversaries now have the ability to seriously impact a nation's information infrastructure and security. In fact, technological sophistication and reliance on information can be a significant center of gravity. So the question is, how do we minimize the vulnerabilities and what responses are available to us? However, before addressing these questions let's look at what some of these threats are and the potential havoc they can cause.

## Notes

[1] R.E. Dupuy and T.N. Dupuy, *The Encyclopedia of Military History* (New York: Harper & Row, 1986), 63.

[2] Ibid., 64.

[3] John Arquilla and David Ronfeldt, "Cyberwar is Coming!," *Comparative Strategy 12*, no. 2 (April-June 1993): 141-165.

[4] Thomas B. Allen, *The Blue and The Gray* (Washington, DC: National Geographic Society, 1992), 54.

[5] Ibid., 54.

[6] Ibid., 57.

[7] Andrew F. Krepinevich, Jr., *The Military-Technical Revolution: A Preliminary Assessment*, Office of the Secretary of Defense, Office of Net Assessment, July 1992.

[8] David Kahn, *The Codebreakers: The Story of Secret Writing* (New York: MacMillan Publishing Co., 1967), 299-300.

[9] David Kahn, *Seizing the Enigma: The Race to Break the German U-Boat Codes, 1939-1943* (Boston: Houghton-Mifflin Co., 1991), ix.

[10] Frederick M. Franks, Jr., "Winning the Information War," *Vital Speeches of the Day LX*, no. 15 (15 May 1994): 453-458.

[11] Alan D. Campen, ed., *The First Information War: The Story of Communications, Computers, and Intelligence Systems in the Persian Gulf War* (Fairfax, VA: AFCEA International Press, 1992).

[12] Martin C. Libicki, *What is Information Warfare?* (Washington, DC: National Defense University Press, 1995), 36-37.

# Chapter 3

# Threats in the Information Age

> *We can only gain the advantage over an enemy by being the first to effectively use offensive and defensive information tactics as part of our warfighting arsenal.*
>
> —Admiral Jeremy M. Boorda
> "Leading the Revolution in $C^4I$," *Joint Forces Quarterly*, Autumn 1995

A major outage of the telephone network occurs, causing extensive failures throughout the East Coast. Shortly thereafter, the West Coast's air traffic control system shuts down, causing huge backups at airports and the potential for disaster. A short while later a significant disruption in several financial market computer systems occurs, causing a major sell-off. Not likely in the US, right? Until recently such occurrences were considered improbable. However, events such as the World Trade Center or the Murrah Federal Building terrorist bombings have changed America's attitude about our immunity to terrorist acts. As rogue states, such as Iraq, Iran, or Libya, gain the capabilities to cause the type of disruption and devastation described above or worse, our vulnerability increases.

As improvements in technology dramatically increased the availability, speed, reliability, and timeliness of information available to a user, the threat associated with

these improvements also increased dramatically. President Clinton stated in his *A National Security Policy of Engagement and Enlargement 1996*:

> In addition, the emergence of the information and technology age presents new challenges to US strategy even as it offers extraordinary opportunities to build a better future. This technology revolution brings our world closer together as information, money and ideas move around the globe at record speed; but it makes possible for the violence of terrorism, organized crime and drug trafficking to challenge the security of our borders and that of our citizens in new ways.[1]

As technologically advanced nations become more and more dependent on information systems for their daily existence, their vulnerability to IW increases. What makes this vulnerability even more ominous is the fact that, unlike previous threats to a nation's security where the adversary could be recognized and confronted, adversaries in the information age will be stealthy and anonymous. Determining whether a rogue state, a "hired" terrorist, or a displeased citizen initiated an act becomes very difficult in today's world. As a result, a nation that would not have previously entertained the thought of attacking a far superior nation, using conventional military weapons, will now find the cover and deception inherent in information age weapons an enticement to engage a superior adversary. Therefore, a nation not prepared to deal with this complex threat will find itself vulnerable to manipulation, distortion, obstruction, or devastation of vital information from computer hackers, terrorist organizations, or disgruntled rogue nations. What are these IW threats?

## Information Warfare Weapons

There are numerous types of information warfare weapons that can disrupt or prevent the flow of vital information. Probably the most frequently identified and utilized IW

weapons are computer viruses. These weapons are easily introduced into a system and can be quite destructive and literally bring an information system to a halt. In his article, *Onward Cyber Soldiers*, Waller describes how the US might respond to a Baghdad, Tehran, or Tripoli who threatens an American ally by injecting a virus into their systems.[2] However, the US is not impervious to this type of warfare as demonstrated by recent intrusions into the Boeing and Justice Department computer systems.[3] Imagine the impact of a virus being introduced into our telephone-switching system or our air traffic control system or our military transportation computer systems. Best case scenario, the virus would cause inconveniences or waste tremendous amounts of manpower trying to find and resolve the problems. Worst case, the havoc created would cause extensive failures, air disasters, or total chaos in a deployment scenario.

To make matters worse a variant of viruses, termed a logic bomb, functions the same as a virus manipulating or destroying software code. However, they are set to activate at a specific time or when a certain condition occurs, potentially weeks or months later. This can provide the culprit total anonymity with the results still the same, computer or communications system failure, or false and potentially lethal information provided. Additionally, an adversary could bribe a manufacturer to insert a logic bomb into a program for a weapon system during production. Once deployed, the weapon looks and feels like a weapon, but the warhead does not explode or it ranges far off target.[4]

Another IW weapon is a non-nuclear electromagnetic pulse (EMP) device. These devices are designed to burn out the electronic components in a computer or communications system, which lead to the same types of problems identified above.[5]

What makes it so difficult to defend against these devices is the fact they can be very small in size and delivered as indiscriminately as a virus or logic bomb.

Have forms of IW begun? Viruses are prevalent throughout the US and the world, infecting systems, causing tremendous investments in manpower, money, and time to find, eradicate, and hopefully, prevent reoccurrence. Hackers, whether for fun or with malicious intent, are constantly invading computer systems. A General Accounting Office study estimates that hackers attack Pentagon computers over 250,000 times per year, with 65 percent having some success in gaining access.[6] In a separate effort by the Defense Information Systems Agency (DISA), DISA personnel penetrated 86 percent of the unclassified DOD computers they attacked with 98 percent of the penetrations not detected.[7] Additionally, Pentagon experts believe outsiders probe military computers about 500 times per day with only a very small percentage being detected.[8] Even worse, the potential exists that for the right money or incentives, hackers may be "bought" by an adversary to conduct IW against our communications, computer, air traffic control, and other systems.

The warfare of the future will look nothing like the conventional warfare of today, with guns, tanks, and bombs. It will resemble something from a James Bond movie or today's virtual reality movies. And, although a technologically advanced country like the US could wage a very effective IW campaign, senior officers believe we need to "take a bite out of the reality sandwich"[9] and realize an enemy, whether technologically advanced or not, bent on disrupting or destroying US capabilities, has access to or can develop tremendously sophisticated IW weapons. In 1994, members of a Pentagon Defense

Science Board (DSB) panel warned of the potential severity of an information attack on the US. They stated,

> This threat arises from terrorist groups or nation states, and is far more subtle and difficult to counter than the more unstructured but growing problem caused by hackers. The threat causes concern over the spectre of military readiness problems caused by attacks on DOD computer systems, but goes well beyond DOD...A large, structured attack with strategic intent against the US could be prepared and exercised under the guise of unstructured activities.[10]

The panel goes on to state the real concern is the US might not even know it is under attack and that "there is no nationally coordinated capability to counter or even detect a structured threat."[11]

The US currently possesses tremendous capabilities to wage an effective IW campaign against an adversary, but as the DSB highlights, the threat is growing in numbers and sophistication and we cannot ignore the reality that we are vulnerable to hostile IW attacks that will be difficult to detect and counter. In large measure we have created this vulnerability ourselves by basing more and more critical capabilities on inadequately protected information systems.[12] From a military perspective, one thing we can do to address the DSB's concerns about crippling operational readiness and military effectiveness is to understand the implications of IW on operations and our ability to meet national objectives. In today's world, where an adversary may be hard to determine and where the US armed forces are being thrust into politically and diplomatically complex missions, providing astute guidance is imperative to ensure adequate preparation and appropriate response. One such mechanism to help provide this sound guidance is to provide definitive rules of engagement.

## Notes

[1] US President, *A National Security Strategy of Engagement and Enlargement, 1996*, (Washington, DC: US Government Printing Office, 1996), 1.

[2] Douglas Waller, "Onward Cyber Soldiers," *Time 146*, no. 8 (Aug. 21, 1995): 39.

[3] CNN news report, 3 Mar 97 (Note: The Boeing break-in cost over $100,000 to verify aircraft design data integrity. The Justice Department break-in embedded racists comments and graphics into their system).

[4] Waller, 41.

[5] Waller, 41.

[6] Peter Grier, "At War with Sweepers, Sniffers, Trapdoors, and Worms," *Air Force Magazine 80*, no. 3 (March 1997): 23.

[7] US Department of Defense, *Report of the Defense Science Board Task Force on Information Warfare-Defense*, Washington, DC: Office of the Under Secretary of Defense (Acquisition and Technology), (November 1996), 2-15.

[8] Waller, 44.

[9] Waller, 43.

[10] US Department of Defense, *Report of the Defense Science Board Summer Study Task Force on Information Architecture for the Battlefield*, Washington, DC: Office of the Under Secretary of Defense (Acquisition and Technology), (October 1994), 24-25.

[11] Ibid., 25.

[12] US Department of Defense, *Report of the Defense Science Board Task Force on Information Warfare-Defense*, 2-2.

# Chapter 4

# Rules of Engagement and International Law's Effects

> *We must use military force selectively, recognizing that its use may do no more than provide a window of opportunity for a society—and diplomacy—to work. We; therefore, will send American troops abroad only when our interests and our values are sufficiently at stake…When we do so, it will be with clear objectives to which we are firmly committed and—when combat is likely—we have the means to achieve decisively. These requirements are as pertinent for humanitarian and other nontraditional interventions today as they were for previous generations during prolonged world wars.*
>
> —President Clinton
> *A National Security Strategy of Engagement and Enlargement*
> February 1996

As President Clinton's comments indicate, we must develop rules of engagement we can tailor to the situation, be it peacetime, military operations other than war (MOOTW), or major contingencies. He further states, "The dangers we face today are more diverse. Ethnic conflict is spreading and rogue states pose a serious danger to regional stability in many corners of the globe. The proliferation of weapons of mass destruction represents a major challenge to our security."[1] And, although IW weapons may not cause the loss of property or human life associated with weapons of mass destruction, IW weapons can bring about great havoc and confusion and seriously impair military readiness. Therefore, how do we effectively deal with this potentially new form of hostility? When is force appropriate and at what level when IW is involved? Are we justified in responding to a

rogue state that acquires the technology and wages an IW campaign against the US? All these questions raise new concerns that may impact the development of rules of engagement (ROE) and appropriate responses to IW activities. Let's begin to address these concerns by first looking at what ROE are, their intent, and what impacts their development.

## Rules of Engagement

ROE provides the guidance and limitations to ensure our military forces are aware of the proper conduct and response levels appropriate and proportional to the mission objectives. Paramount in ROE development is the rules not be so restrictive as to hinder mission accomplishment or increase the risk to personnel, while always ensuring and emphasizing the right to self-defense.[2] Article 51 of the UN Charter asserts the inherent right of individual or collective self-defense if an armed attack occurs.[3] There is a fine line between ensuring self-defense and providing the guidance necessary to minimize escalation of hostilities. Our troops must know their protection and right to self-defense is a matter of utmost importance and that we weighed all available intelligence, international law, and potential consequences carefully.[4] As a result, we must have ROE that are flexible enough to effectively address any situation, throughout the peacetime/conflict continuum. This line becomes even finer when IW enters the picture and creates new and challenging problems for our commanders. For example, prior to the outbreak of hostilities, efforts to prep the battlefield could include intelligence-gathering efforts to discern enemy capabilities; accessing their computer systems; or placing non-lethal, destructive signatures in their information systems for activation at a later date.[5]

To deal effectively and appropriately with these challenges, ROE must be flexible, clear, and concise in their purpose, while taking into account all the factors that impact ROE development. Rules of engagement are effective only to the extent they are understood and appropriately applied. Elements that help define the appropriate application of ROE are depicted in Figure 2.

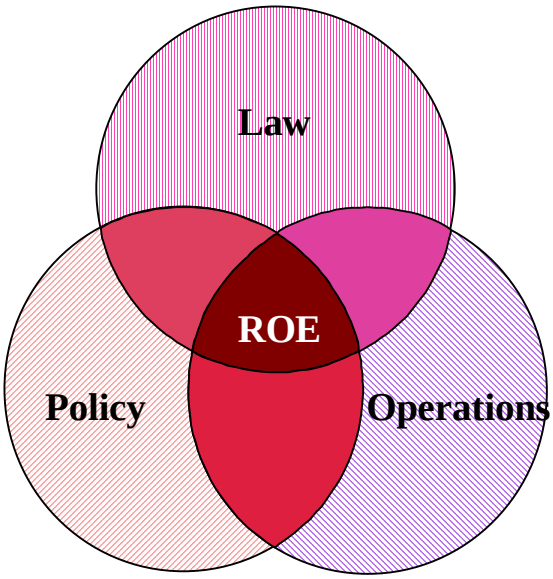


**Figure 2. Elements that Affect the Basis of ROE**

We cannot anticipate every situation, but ROE should provide all levels of command with the intent of the ROE as well as ensure the fielded forces understand the mission and the importance of appropriate action and restraint, while not minimizing the right to self-defense.[6] If ROE are not sufficient to provide guidance for a given situation, the leadership must take the initiative to modify and receive approval to change the ROE, as necessary, to accommodate a situation.

To assist commanders in developing ROE, the Joint Chiefs of Staff issued the Standing Rules of Engagement (SROE) which contains the basic rules of self-defense and the application of force for mission accomplishment pertinent to any situation.[7] It

provides combatant commanders the latitude to modify the SROE, depending on the situation, and subordinate commanders the ability to request supplemental measures. Inherent in the SROE are the following elements:[8]

> *Necessity*—A hostile act occurs or a force or terrorist unit exhibits hostile intent.
>
> *Proportionality*—The force used must be reasonable in intensity, duration, and magnitude, based on all facts known to the commander at the time, to decisively counter the hostile act or hostile intent and to ensure the continued safety of US forces.

Many factors affect rules of engagement and their development must address policy, operational, and legal factors to ensure our forces understand their right to self-defense, while also taking into account mission accomplishment and the elements of proportional, appropriate response. Also, they must be unambiguous and written so everyone knows they will not be prosecuted if they abide by the ROE. This is critical because as our military forces become involved in more and varied situations, such as IW scenarios, the transition from peacetime to conflict becomes clouded. Therefore, decisions and preparations made to address these various situations can have serious consequences on post-hostility efforts and the future world end-state. As depicted in figure 2, one element of critical importance to consider in developing ROE is the legal element.

## Legal Considerations: Now and in the Future

The primary legal force affecting ROE development is international law. International law is law that influences how countries and recognized international organizations conduct themselves; it does not govern individual conduct.[9] These laws are primarily of two types. The first is treaty law, written or oral agreements entered into by authorized

representatives; examples include the Geneva Convention and Hague Laws. It is important to note treaty law is only binding on the signatories and; therefore, creates problems when determining violations of international law. In short, a state that does not sign the treaty is not bound to its articles. The second type, customary law, is based on a nation's consistent practices and is viewed by other nations as legally binding; examples include the Law of Land Warfare and the Law of the Sea.[10]

One major subcategory of international law is the law of armed conflict (LOAC). The LOAC attempts to minimize suffering and destruction by controlling the effects of hostilities through minimum standards of conduct, protection to both combatant and noncombatants, and the promoting of peace at the end of hostilities. As a result, US compliance with the LOAC is a legal must to avoid international condemnation, and; therefore, the development of our ROE must comply with the LOAC. DOD Directive 5100.77, DOD Law of War Program, and Air Force Policy Directive 51-4, Compliance with the Law of Armed Conflict, state the US will comply with the LOAC and report any violations.[11]

Just as our ROE must comply with the LOAC and international laws, there are other legal considerations. First, ROE must comply with US domestic laws, such as the Uniform Code of Military Justice, and the moral guidance in the Code of Conduct.[12] Second, in developing ROE, the laws of host nations and our allies are critical factors to consider.[13] Third, a nation's position regarding their neutrality is an important consideration. Failure to consider these in developing our ROE could have serious effects from a legal, moral, and international standpoint. So, how do we ensure compliance?

## Basic Principles of the Law of Armed Conflict

To adequately comply with the LOAC, we must first be aware of certain basic principles contained in the LOAC. These principles are:[14]

> *Proportionality.* Use force no greater than necessary to accomplish legitimate military objectives. It also seeks to prevent forces from attacking in situations where civilian casualties would outweigh military gains.
>
> *Military Necessity.* Permits only that degree of regulated force required for partial or complete submission of the enemy with the least expenditure of life, time, and physical resources.
>
> *Humanity.* Prohibits the employment of any kind or degree of force not necessary for the purposes of war. Requires any nation desiring to implement a new type of weapon to make a determination, prior to its use, regarding its compliance with the principle of humanity.
>
> *Chivalry.* Waging of war in accordance with well-recognized formalities and courtesies.

Prior to efforts to codify the acceptable conduct of war, the only factors that impacted how armies fought were the codes of chivalry that existed and the level of benevolence of the commanders. Short of these factors, armies fought conflicts with little consideration for proportionality or necessity. The objective was to destroy the enemy by whatever means available.

However, these basic principles directly impact our ROE development. First, we are morally and legally obligated to observe the LOAC and the values and principles contained in it. Second, we go to great lengths to conduct operations in a manner that reflects our values and principles and which we want other nations to embrace. Therefore, it is paramount we ensure our troops follow the law and conduct themselves appropriately so that we do not damage our image in the international community's eyes. However,

understanding and complying with international law is somewhat easier in a conflict scenario where the rules are more clearly defined and the adversaries, in most cases, are known. But how does international law affect situations where non-lethal weapons and discriminate technologies are used?

One can easily imagine situations where the LOAC and its associated principles may not be totally applicable to a given scenario. For example, what about in peace operations, such as humanitarian assistance or MOOTW, where a rogue nation or faction wages an IW campaign against the US; what principles apply, what responses are available to us? How does the international legal system apply, if at all?

The basis in developing ROE for MOOTW, conflict, or IW scenarios should differ little. Rules of engagement provide guidance that defines how we operate and restrictions imposed to reduce the chances for escalation of hostilities. What is different is the context within which the rules are tailored. In conflict situations, attacks are restricted by the LOAC and the previously discussed principles as well as our government's policies. However, in peacetime the CJCS Standing Rules of Engagement state that attacks should only be in self-defense, that is, against use of force, threat of imminent use of force, and continuing threat of use of force.[15]

Recognizing IW can occur in either a wartime or peacetime scenario, should the LOAC, international agreements, or treaties apply to IW? I believe the answer is, yes. When conducted, if the intent is to jeopardize national security interests, we should evaluate and apply LOAC principles and international treaties to develop an informed, appropriate response. However, with today's technology and the sophistication of IW threats, the ability to identify a combatant, a noncombatant, and an unlawful combatant are

critical elements to develop a response. The Geneva Convention describes each as follows:[16]

> *Combatant*. An individual authorized by government authority or the LOAC to engage in hostilities. (For example, regular armed forces)
>
> *Noncombatant.* An individual not authorized by governmental authority or the LOAC to engage in hostilities and does not engage in hostilities. (For example, civilians, POWs, and chaplains)
>
> *Unlawful combatant*. An individual who is unauthorized by governmental authority or the LOAC to engage in hostilities but does engage in hostilities.

The real problem, from an IW standpoint and determining what should be an appropriate response to a nation's apparent IW campaign, is due to the stealthy nature of IW weapons; determining who are combatants, unlawful combatants, and who are neutral; and what is the intent. Information warfare attacks can leave no "fingerprints" as to from whom, when, or where the IW attack emanated. Identifying the perpetrator, and determining whether a nation sponsored the IW attack and their intent could be very difficult. For example, was the person "hired" by an adversary, was the person acting unilaterally in support of their nation, or was the person just hacking? These are questions not easily answered, but dealing appropriately with them is a challenge for decision makers and commanders in developing ROE and responses. The comprehensiveness of the developed ROE can have serious repercussions on the desired end-state and level of retaliation. As a result, we must train our commanders and provide our troops with pro and con guidance to ensure appropriate, proportional response within legal constraints.

The Law of Armed Conflict is a good starting point for developing ROE that are applicable to potential IW scenarios. Additionally, we must consider whether the US is a signatory of any international agreements. For example, the US is a signatory of the

International Telecommunications Satellite Organization (INTELSAT) Agreement which provides specialized telecommunications services, but only for non-military purposes.[17] Also, information systems operated by other nations may not be accessible because of a nation's declared neutrality. What this means is we cannot traverse a neutral nation's information infrastructure to wage IW on another country; this is a violation of their neutrality.

Another consideration is the military's ever expanding use of commercial information systems. As the LOAC principle of necessity implies, if a commercial system supports the accomplishment of a military mission, is it a valid target from a military perspective? Because of the increasing interdependencies and sharing of telecommunications lines, the delineation between military and civilian information systems is becoming virtually impossible to separate. As a result, determining the motive of an IW attack is difficult and will impact our response(s).

In summary, the specifics of IW, appropriate responses, and further ROE refinement will gradually develop as new, more virulent forms of IW occur. The tremendous dependence on information and the blurring of lines between military and civilian systems makes the ability to appropriately respond to an IW attack very difficult. Additionally, determining the actors and their motives will be very difficult, especially as IW tactics become more sophisticated. However, it is a process and an eventuality we must plan for and be prepared to respond to should we become victims of an IW attack.

## Notes

[1] US President, *A National Security Strategy of Engagement and Enlargement, 1996*, (Washington, DC: US Government Printing Office, 1996), 1.

## Notes

[2] CDR Butch Thompson, "Factors Influencing Rules of Engagement, and ROE's Effect on Mission," Naval War College research paper, 16 May 1995, 1.

[3] Col. Jack L. Rives, et al., *The Military Commander and the Law*, 3rd Edition, 1996, (Air Force Judge Advocate General School, Maxwell AFB, AL), 542.

[4] Joint Warfighting Center, *Joint Task Force Commander's Handbook for Peace Operations*, 28 February 1995, 75.

[5] "A Primer on Legal Issues in Information Warfare," lecture, Information Warfare Symposium, Maxwell AFB, AL., 21-23 October 1996.

[6] Headquarters, Dept. of the Army, *FM-100-23, Peace Operations*, 30 December 1994, 35.

[7] Col. Jack L. Rives, et al., 542.

[8] LCDR Scott Edward Smith, "What Factors Affect Rules of Engagement for Military Operations Other Than War?," Naval War College research paper, 13 February 1995, 7.

[9] Col. Jack L. Rives, et al., 529.

[10] Ibid., 530-531.

[11] Ibid., 535.

[12] Ibid., 536.

[13] Ibid., 541

[14] Ibid., 538, 561-562.

[15] Ibid., 543.

[16] Ibid., 537-538.

[17] Ibid., 562.

# Chapter 5

# Conclusions

> *The promise of infowar has grown exponentially with the increasing power and pervasiveness of computer microprocessors, high-speed communications, and sophisticated sensors…The potential for low-cost and bloodless solution of conflicts brings with it other problems.*
>
> —Douglas Waller
> "Onward Cyber Soldiers," *Time*, 21 August 1995

Since the beginning of warfare, the intent has been to physically and psychologically destroy an adversary. Little consideration was given to the amount of destruction caused to a country's infrastructure or loss of human life. In most cases, ROE were not codified, but left to the commander's discretion on how to conduct the war. However, as man refined warfighting, we codified the rules regarding warfare conduct to limit human suffering and loss of life. The advent of modern, "nonlethal" weapons, such as IW weapons, has the potential to change the way wars will be waged in the future. These "nonlethal" weapons can result in significant destruction and loss of life in large numbers. As a nation that holds the value of human life and freedoms high, the US must prepare to deal with "nonlethal" attacks, which have the capability to not only cause economic chaos and loss of life, but impinge on freedoms we take for granted, yet hold so dear. As a result, when confronted with an IW scenario, whether in peacetime or conflict, we must be

prepared to respond appropriately. However, our responses must comply with various factors, including international laws, treaties, and neutrality considerations.

Whether, in a peacetime or hostile environment, our responses should be no less decisive if an adversary threatens our national security interests. Should an adversary caught waging IW, in "peacetime" to influence policy and affect our national security, be held any less accountable than an adversary who, in "peacetime," explodes a bomb in a German nightclub, an aircraft in midair, or a building killing 240 Marines, with the same objectives? If someone threatens our national security interests, we must be prepared to respond, within legal limits, to defend those freedoms we value. Aside from developing methods of identifying IW attacks on our national security, the major task is to devise an approach to effectively respond to attacks on our security, once we identify the adversary and motive.

## Developing Response Options

A key to any response option is the need to accurately and quickly identify the actor and the motive(s) for the action(s). Knowing the motives of the actor will help determine the jurisdictional and legal environment our response options must consider as well as help define the level of civil-military cooperation required to respond to the IW attack. Also, knowing the actor's motive(s) will allow us to attack the adversary's instrument of power that is proportional to their IW attack on us. As a result, each attack must be analyzed on its own circumstances as similar events may have completely different motives, sponsorship, and severity and therefore, require different responses.[1] Finally, the effectiveness of the response is dependent on the timeliness and efficiency of the detection

capabilities. Timely identification and response will let our adversaries know we have developed the capabilities to identify IW attacks and instill confidence and support in our public for our continued IW efforts.[2]

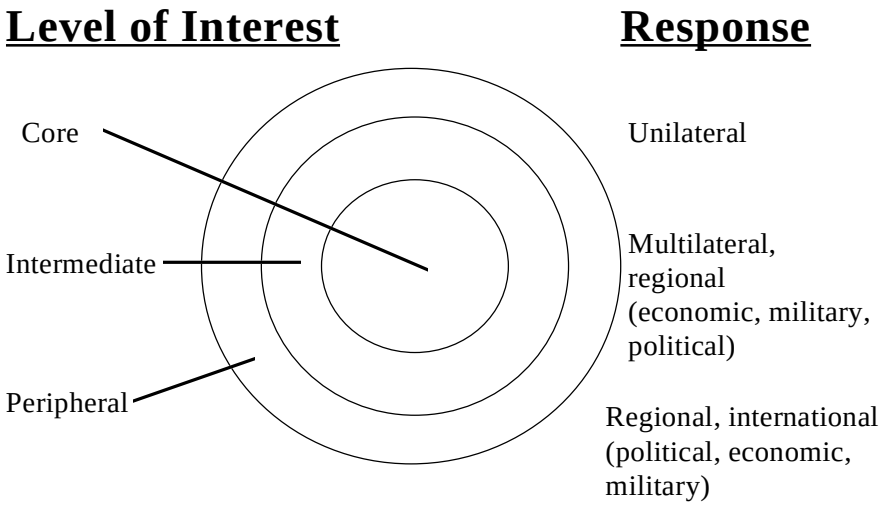


**Figure 3. Interest and Responses Model**

Developing a credible response will influence potential adversaries' perceptions of our resolve and hopefully deter future IW attacks. Figure 3 provides a basis to guide our response options to nations who choose to wage IW on the US. The intent of this model is to provide response options based on the threat to US security interests. For example, core interests are those interests dealing with the physical survival of a country or directly threatening a nation's national security interests or population and should be dealt with unilaterally,[3] within the constraints of international law and the principles of proportionality and necessity. The large, structured IW attack with strategic intent discussed by the Defense Science Board would be such a threat and warrant a unilateral response with the full range of military resources, including the use of offensive IW capabilities.[4] Our response should include parallel IW attacks directed at their military, economic, political, and information infrastructures with the intent to affect the

adversary's will and capacity to wage further IW campaigns. This does not necessarily entail targeting the adversary's military information systems. A more productive response may be to conduct an IW attack on their data systems and infrastructure that provides us a more strategic advantage, such as their air traffic control, financial, or information systems that support their warfighting capabilities. However, before we attack any system, we must conduct a critical analysis to determine their centers of gravity that will provide a cascading effect if attacked, as well as ensure there is no ambiguity in our intent and response.

Threats to our intermediate interests concern our political and economic security. Our responses to IW attacks on our intermediate interests should be more coalition oriented, with retaliatory IW attack options being utilized only after we exhaust our political and economic options.[5] However, if an IW attack is required, we should respond with appropriate offensive IW capabilities. In other words, attack the adversary with proportional force, disruption, and destruction to their national infrastructure as the intent of their IW attack on us. Because attacks on our intermediate interests would include attacking our economic and political security, our responses should be directed primarily against similar targets. Again, knowing the adversary's intent will provide the basis for our proportional response. An example of a US response to attacks on our intermediate interests occurred when we identified Libya as the state primarily responsible for sponsoring the terrorist bombing of a German nightclub. The US responded by conducting Operation El Dorado Canyon to let Libya know we would not tolerate this threat to our national security or those of our allies.

Finally, threats to our peripheral interests concern sociopolitical, humanitarian, religious, and cultural problems.[6] Our response to IW attacks on our peripheral interests should initially involve the use of nonmilitary means, such as our political and economic instruments of power.[7] However, if a military response is judged necessary, it should be to utilize the unique capabilities the military possesses and, if necessary, be a coalition effort targeted against only those areas that affect our national interests. Also, as with threats to our core and intermediate interests, our response must be proportional to the adversary's intent and threat. Primary in the decision on how to respond militarily is the level of threat to our vital interests as well as the costs and risks associated with using our military.[8]

How is a nation that wages an IW campaign on our military computer systems and disrupts our military readiness or threatens our national sovereignty, primarily to influence policies, any different than a nation who bombs a nightclub, killing dozens of people with the same intent? Should our responses be any different? The method used to try and sway policy or compromise security is irrelevant; it is the intent and potential by-product of those efforts that should determine the appropriate response. If a strategic IW attack threatens a nation's sovereignty and physical existence, the level of response should be similar whether in a conventional or an IW environment.

When IW is waged against US interests and security aspects, the appropriate response, once we identify the perpetrator and their motives, should be based on the degree of threat to national security, while also considering the political, operational, and legal elements. As our national-level information infrastructure becomes more dependent on automated control and information systems, the ability to distinguish between

commercial and military systems will further cloud. An attack on commercial systems, with embedded military systems, will require more interagency and joint military-civil collaboration efforts to provide effective, credible responses. As discussed in *Information Warfare: A Strategy for Peace…A Decisive Edge in War*, the employment of IW capabilities can occur in peacetime to deter a crisis, prevent escalation, project power, or promote peace. However, when employed, approval will require NCA approval, with support, coordination, deconfliction, cooperation, and participation from a variety of agencies to ensure the response meets all the legal and political elements and is a proportional response.[9]

The above responses primarily focus on offensive response options, but to have a comprehensive, credible response package, we must also have a defensive response capability. Critical to an effective defensive IW response is the timely, accurate identification of the intrusion and possible objective of the adversary. Whenever we detect an intrusion, we should assume it has a hostile intent and take the necessary defensive actions to minimize the effects of the attack on our information infrastructure.[10] This defensive response not only provides protection to our information infrastructure and instills confidence in our population, but it serves as a deterrent to possible attackers that we can detect and withstand their IW attempts. Our defensive responses should reflect an incremental tightening of our information infrastructure's defensive posture as the threat increases, based on a pattern of attacks that signifies an IW attack scenario.[11] Paramount to developing an effective defensive response option is the requirement to assess our vulnerabilities as well as to identify those information infrastructures that are our centers of gravity (COGs). We need to put ourselves in a potential adversary's mindset and

critically analyze where we are susceptible to IW attacks and what systems, processes, and databases need defended. Without this assessment, we could spend millions of dollars in security efforts, but still be vulnerable to crippling IW attacks.

## Keys to Effective, Appropriate Responses

The implementation of effective, appropriate responses to IW attacks is just one part of the equation in ensuring we respond appropriately to IW attacks. A second part of the response process is to ensure commanders and troops understand the legal ramifications associated with the IW environment, both internationally and domestically. The IW environment is a complex, rapidly changing one that requires trained decision makers and troops to deal with the myriad of situations they will potentially encounter.

One element to help ensure they are able to operate in this complex environment is to develop education and training programs that focus on IW concepts; legal issues; protection, detection, and reprisal tactics; and roles of IW throughout the spectrum of military operations. This program should also focus on heightening awareness of the threats and vulnerabilities. Providing decision makers and troops with this knowledge will help develop effective, concise ROE that comply with the LOAC and international and domestic laws as well as a more informed group of personnel to advance effective, innovative offensive and defensive approaches to the IW threat.

Another element to help develop an effective response program should be the inclusion of IW scenarios in our exercises and wargaming simulations. Providing decision makers and troops with real-world IW scenarios will provide the benefits of exercising the ROE developed to respond to IW attacks, provide opportunities to modify ROE as

situations occur, and test response options for their compliance with legal aspects and outcomes. Exercises also afford the advantage of providing opportunities to learn lessons that will further enhance the development of effective, flexible ROE and appropriate offensive and defensive response options.

A third element to an effective response program is to develop a strategy for dealing with IW attacks. This program should include a vulnerability assessment of essential information processes and functions that need restored quickly to prevent the loss of basic, critical functions.[12] Not only does this help provide the groundwork for developing a credible defensive response option, but also serves as a deterrent to adversaries by demonstrating our ability to effectively manage critical information systems while under an IW attack.

## Areas for Future Research

The impact of international law on information warfare is only now beginning to receive attention. This is an area that will continue to mature over the next several years as situations arise that force more emphasis in this area. However, there are other areas concerning IW that present equally valuable research areas and which we should start to address.

First, we should start to look at what information infrastructures need defended. In other words, what are our critical information centers of gravity (COGs); including both military and non-military information systems. This research should focus on vulnerabilities and developing a minimum essential set of information systems to protect.

This list is critical for developing a defensive response option to IW attacks and could serve as a deterrent to potential adversaries.

A second area for future research entails developing a strategy to defend our essential information COGs. It is technically and economically impractical to defend our entire information infrastructure against all attacks. By developing a comprehensive defense strategy, we can better manage the risks to our national information infrastructure and national security. This strategy should include a matrix that associates required defensive responses to a threat condition.

A third area for future research concerns looking at how other countries deal with an adversary who "attacks" their information systems. In other words, what laws do other countries have in place to address IW attacks; how do they define combatant, noncombatant, and unlawful combatant; and how would they respond to and what is their philosophy concerning IW attacks? This has definite importance for the US as our national information infrastructures become more tightly interconnected with the global information infrastructure. Knowing how other countries are addressing the legal aspects of IW and how they would respond to IW attacks not only helps us devise an IW strategy, but will enhance our national and military preparedness to legally and appropriately respond to IW attacks.

IW is a fact of life in today's society and military. Its impact will continue to expand and affect all levels of military operations. Information is a strategic, vital resource to our national security and to the effective operation, deployment, and employment of our military.[13] Having leaders and troops trained to understand the IW environment, the threats and vulnerabilities they face, and the legal aspects they must address, will ensure

our ROE and responses are appropriate and comply with international legal factors. It is critical this training and knowledge permeates throughout the military as our warfighters become more dependent on information and information systems. The US must prepare to effectively respond to any IW threat; failure to do so could lead to inappropriate responses, escalation of hostilities, and ultimately, unacceptable end states.

## Notes

[1] Office of the Joint Chiefs of Staff, "Information Warfare: A Strategy for Peace... The Decisive Edge in War," 11-12.

[2] Ibid., 11.

[3] Dr. Karl P. Magyar, "Conflict in the Postcontainment Era," *War and Conflict Coursebook*, ACSC AY97, 14.

[4] US Department of Defense, *Report of the Defense Science Board Summer Study Task Force on Information Architecture for the Battlefield*, Washington, DC: Office of the Under Secretary of Defense (Acquisition and Technology), (October 1994), 24.

[5] Dr. Karl P. Magyar, 14.

[6] Ibid., 14.

[7] Ibid., 14.

[8] US President, *A National Security Strategy of Engagement and Enlargement*, 1996, (Washington, DC: US Government Printing Office, 1996), 18.

[9] Office of the Joint Chiefs of Staff, 13.

[10] US Department of Defense, *Report of the Defense Science Board Task Force on Information Warfare-Defense*, Washington, DC: Office of the Under Secretary of Defense (Acquisition and Technology), (November 1996), 6-27.

[11] Ibid., Appendix C.

[12] Ibid., 4-1 and 4-2.

[13] Office of the Joint Chiefs of Staff, 1.

## *Bibliography*


*A Primer on Legal Issues in Information Warfare*. Lecture. Information Warfare Symposium. Maxwell AFB, AL. 21-23 October 1996.

Allen, Thomas B. *The Blue and The Gray*. Washington, DC: National Geographic Society, 1992.

Arquilla, John, and David Ronfeldt. "Cyberwar is Coming!" *Comparative Strategy 12*, no. 2 (April-June 1993): 141-165.

Campen, Alan D., ed. *The First Information War: The Story of Communication, Computers, and Intelligence Systems in the Persian Gulf War*. Fairfax, VA: AFCEA International Press, 1992.

Dupuy, R.E., and T.N. Dupuy. *The Encyclopedia of Military History*. New York: Harper & Row, 1986.

Franks, Frederick M., Jr. "Winning the Information War." *Vital Speeches of the Day LX*, no. 15 (15 May 1994): 453-458.

Gertz, Bill. "Terrorism and the Force." *Air Force Magazine 80*, no. 2 (February 1997): 71.

Grier, Peter. "At War with Sweepers, Sniffers, Trapdoors, and Worms." *Air Force Magazine 80*, no. 3 (March 1997): 23.

Headquarters, Department of the Army. Army Manual (FM) 100-23. *Peace Operations*, 30 December 1994.

Joint Warfighting Center. *Joint Task Force Commander's Handbook for Peace Operations*, 28 February 1995.

Kahn, David. *Seizing the Enigma: The Race to Break the German U-Boat Codes, 1939-1943*. Boston: Houghton-Mifflin Co., 1991.

———. *The Codebreakers: The Story of Secret Writing*. New York: MacMillan Publishing Co., 1967.

Krepinevich, Andrew F., Jr. *The Military-Technical Revolution: A Preliminary Assessment*. Office of the Secretary of Defense, Office of Net Assessment, July 1992.

Libicki, Martin C. *What is Information Warfare?*. Washington, DC: National Defense University Press, 1995.

Lubar, Steven. *Infoculture*. Boston: Houghton Mifflin Co., 1993.

Magyar, Dr. Karl P. "Conflict in the Postcontainment Era." *War and Conflict Coursebook*. (AY97): 14.

Office of the Joint Chiefs of Staff. *Information Warfare: A Strategy for Peace...The Decisive Edge in War*. 1996.

Powell, General Colin L. "Information-Age Warriors." *Byte 17*, (July 1992): 370.

Rives, Col Jack L., et al. *The Military Commander and the Law.* 3rd Edition. Air Force Judge Advocate General School: Maxwell AFB, AL, 1996.

Smith, LCDR Scott Edward. “What Factors Affect Rules of Engagement for Military Operations Other Than War?” Naval War College research paper. (13 February 1995): 7.

Thompson, CDR Butch. “Factors Influencing Rules of Engagement, and ROE’s Effect on Mission.” Naval War College research paper. (16 May 1995): 1.

US Department of Defense. *Report of the Defense Science Board Task Force on Information Warfare-Defense.* Washington, DC: Office of the Under Secretary of Defense (Acquisition and Technology), November 1996.

US Department of Defense. *Report of the Defense Science Board Summer Task Force on Information Architecture for the Battlefield.* Washington, DC: Office of the Under Secretary of Defense (Acquisition and Technology), October 1994.

US President. *A National Security Strategy of Engagement and Enlargement,*1996. Washington, DC: US Government Printing Office, 1996.

Waller, Douglas. “Onward Cyber Soldiers.” *Time 146,* no. 8 (21 August 1995): 39-44.

DISTRIBUTION A:

Approved for public release; distribution is unlimited.

Air Command and Staff College
Maxwell AFB, Al 36112